7 marks question unit 1

1. What are the different communication modes? Give example for each.

Transferring data between two devices is known as a communication mode. Buses and

networks are designed to allow communication to occur between individual devices that

are interconnected.

Simplex transmission

In simplex transmission mode, the communication between sender and receiver occurs

in only one direction. The sender can only send the data, and the receiver can only

receive the data. The receiver cannot reply to the sender.

Ex:

• Simplex transmission can be thought of as a one-way road in which the traffic travels

only in one direction—no vehicle coming from the opposite direction is allowed to

drive through.

• To take a keyboard/monitor relationship as an example, the keyboard can only send

the input to the monitor, and the monitor can only receive the input and display it on

the screen. The monitor cannot reply, or send any feedback, to the keyboard.

Half Duplex

The communication between sender and receiver occurs in both directions in half-duplex

transmission, but only one at a time. The sender and receiver can both send and receive

the information, but only one is allowed to send at any given time. Half-duplex is still

considered a one-way road, in which a vehicle travelling in the opposite direction of the

traffic has to wait till the road is empty before it can pass through.

Ex:

For example, in walkie-talkies, the speakers at both ends can speak, but they have to

speak one by one. They cannot speak simultaneously.

Full Duplex

In full-duplex transmission mode, the communication between sender and receiver can

occur simultaneously. The sender and receiver can both transmit and receive at the

same time. The full-duplex transmission mode is like a two-way road, in which traffic can

flow in both directions at the same time.

Ex:

For example, in a telephone conversation, two people communicate, and both are free

to speak and listen at the same time.

3. Give ISO/OSI reference model for computer communication?

The International Organization for Standardization (ISO) developed the OSI reference

model. The Open Systems Interconnection (OSI) model describes seven layers that

computer systems use to communicate over a network.

The OSI model is the primary architectural model for networks. It describes how data

and network information are communicated from applications on one computer,

through the network media, to an application on another computer. The OSI reference

model breaks this approach into layers.

The OSI reference model has seven layers:

• The Application layer

• The Presentation layer

• The Session layer

• The Transport layer

• The Network layer

• The Data Link layer

• The Physical layer

7. Application Layer

The application layer is used by end-user software such as web browsers and email

clients. It provides protocols that allow software to send and receive information and

present meaningful data to users. A few examples of application layer protocols are the

Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol

(POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

6. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices

should encode, encrypt, and compress data so it is received correctly on the other end.

The presentation layer takes any data transmitted by the application layer and prepares

it for transmission over the session layer.

5. Session Layer

The session layer creates communication channels, called sessions, between devices. It is

responsible for opening sessions, ensuring they remain open and functional while data is

being transferred, and closing them when communication ends. The session layer can

also set checkpoints during a data transfer—if the session is interrupted, devices can

resume data transfer from the last checkpoint.

4. Transport Layer

The transport layer takes data transferred in the session layer and breaks it into

“segments” on the transmitting end. It is responsible for reassembling the segments on

the receiving end, turning it back into data that can be used by the session layer. The

transport layer carries out flow control, sending data at a rate that matches the

connection speed of the receiving device, and error control, checking if data was

received incorrectly and if not, requesting it again.

3. Network Layer

The network layer has two main functions. One is breaking up segments into network

packets, and reassembling the packets on the receiving end. The other is routing packets

by discovering the best path across a physical network. The network layer uses network

addresses (typically Internet Protocol addresses) to route packets to a destination node.

2. Data Link Layer

The data link layer establishes and terminates a connection between two physicallyconnected nodes on a network. It breaks up packets into frames and sends them from

source to destination. This layer is composed of two parts—Logical Link Control (LLC),

which identifies network protocols, performs error checking and synchronizes frames,

and Media Access Control (MAC) which uses MAC addresses to connect devices and

define permissions to transmit and receive data.

1. Physical Layer

The physical layer is responsible for the physical cable or wireless connection between

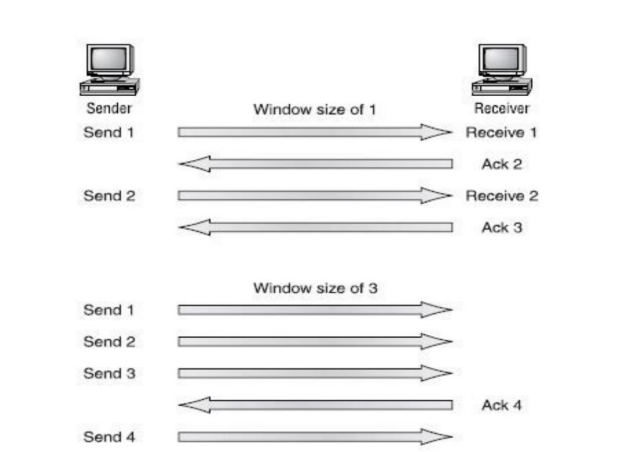
network nodes. It defines the connector, the electrical cable or wireless technology

connecting the devices, and is responsible for transmission of the raw data, which is

simply a series of 0s and 1s, while taking care of bit rate control.

4. Explain sliding window protocol for flow control between sending and receiving with a

window size 3?



Data throughput would be low if the transmitting machine had to wait for an

acknowledgment after sending each segment. Because there’s time available after the

sender transmits the data segment and before it finishes processing acknowledgments

from the receiving machine, the sender uses the break to transmit more data. The

quantity of data segments the transmitting machine is allowed to send without receiving

an acknowledgment for them is called a window. Windowing controls how much

information is transferred from one end to the other. While some protocols quantify

information by observing the number of packets, TCP/IP measures it by counting the

number of bytes.

In the figure there is a window size of 1 and a window size of 3. When a window size of 1

is configured, the sending machine waits for an acknowledgment for each data segment

it transmits before transmitting another.

Configured to a window size of 3, it’s allowed to transmit three data segments before an

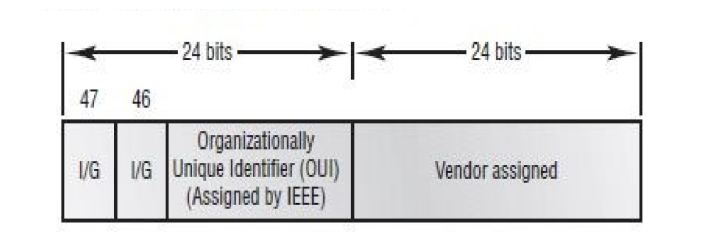
acknowledgment is received. In our simplified example, both the sending and receiving

machines are workstations. Reality is rarely that simple, and most often

acknowledgments and packets will commingle as they travel over the network and pass

through routers.

8. Explain the Ethernet addressing with diagram.



Ethernet addressing uses the Media Access Control (MAC) address burned into each and

every Ethernet Network Interface Card (NIC). The MAC address, sometimes referred to

as a hardware address, is a 48-bit address written in a canonical format to ensure that

addresses are at least written in the same format, even if different LAN technologies are

used. Figure 1.10 shows the 48-bit MAC addresses and how the bits are divided.

The Organizationally Unique Identifier (OUI) is assigned by the IEEE to an organization

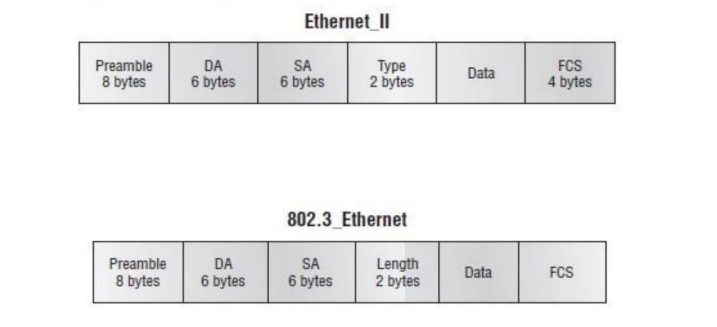
(24 bits or 3 bytes). The organization, in turn, assigns a globally administered address (24

bits or 3 bytes) that is unique (supposedly) to each and every adapter they manufacturer.

Notice bit 46. Bit 46 must be 0 if it is a globally assigned bit from the manufacturer and 1

if it is locally administered from the network administrator.

9. Explain structure of Ethernet frame format as per IEEE 802.3 standard.



Preamble: An alternating 1,0 pattern provides a 5MHz clock at the start of each packet,

which allows the receiving devices to lock the incoming bit stream. The preamble uses

either an SFD or synch field to indicate to the receiving station that the data portion of

the message will follow.

Start Frame Delimiter (SFD)/Synch: SFD is 1,0,1,0,1,0, etc., and the synch field is all 1s.

The preamble and SFD/synch field are 64 bits long.

Destination Address (DA): This transmits a 48-bit value using the Least Significant Bit

(LSB) first. DA is used by receiving stations to determine if an incoming packet is

addressed to a particular node. The destination address can be an individual address, or

a broadcast or multicast.

Source Address (SA): SA is a 48-bit MAC address supplied by the transmitting device. It

uses the Least Significant Bit (LSB) first. Broadcast and multicast address formats are

illegal within the SA field.

Length or Type field: 802.3 uses a length field, whereas the Ethernet frame uses a type

field to identify the Network layer protocol. 802.3 cannot identify the upper-layer

protocol and must be used with a proprietary LAN, for example, IPX.

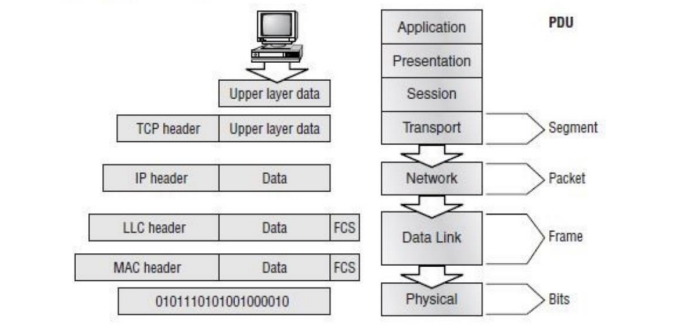
Data: This is a packet sent down to the Data Link layer from the Network layer. The size

can vary from 46–1500 bytes.

Frame Check Sequence (FCS): FCS is a field at the end of the frame

that is used to store the cyclic redundancy check (CRC).

10. What is data encapsulation? Explain with diagram?



When a host transmits data across a network to another device, the data is encapsulated

with protocol information at each layer of the OSI model. Each layer communicates only

with its peer layer on the receiving device.

To communicate and exchange information, each layer uses what are called Protocol

Data Units (PDUs). These hold the control information attached to the data at each layer

of the model, which is typically attached to the header of the data field but can also be in

the trailer, or end of the data field.

Each PDU is attached to the data by encapsulating it at each layer of the OSI model. Each

PDU has a specific name depending on the information each header has. This PDU

information is only read by the peer layer on the receiving device and then is stripped off

and the data is handed to the next upper layer.

At a transmitting device, the data encapsulation method works as follows:

1. User information is converted to data for transmission on the network.

2. Data is converted to segments and a reliable connection is set up between the

transmitting and receiving hosts.

3. Segments are converted to packets or datagrams, and a logical address is placed in the

header so each packet can be routed through an inter- network.

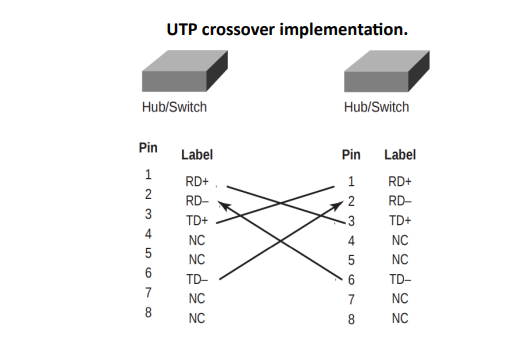
4. Packets or datagrams are converted to frames for transmission on the local network.

Hardware (Ethernet) addresses are used to uniquely identify hosts on a local network

segment.

5. Frames are converted to bits, and a digital encoding and clocking scheme is used.

12. What is cross over cable? give the different use of cross over cables used?



In the implementation of a crossover, the wires on each end of the cable are crossed.

Transmit to Receive and Receive to Transmit on each side, for both tip and ring.

UTP crossover implementation.

Notice that pin 1 on one side connects to pin 3 on the other side, and pin 2 connects to

pin 6 on the opposite end.

You can use a crossover cable for the following tasks:

• Connecting uplinks between switches

• Connecting hubs to switches

• Connecting a hub to another hub

• Connecting a router interface to another router interface

• Connecting two PCs together without a hub or switch

1. marks unit 1

1. Give ISO/OSI reference model for computer communication?

Ans Same as question 3 of 7 marks

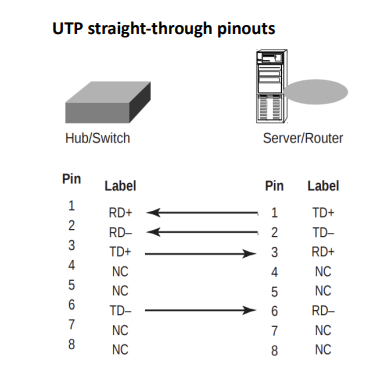
2. Explain sliding window protocol for flow control between sending and receiving with a

window size 3?

Ans Same as question 4 of 7 marks

3. Give the pin connection to create a Straight Through and Cross Over and Roll Over Cable along

with its usages.



In a UTP implementation of a straight-through cable, the wires on both cable ends are in

the same order. Below figure shows the pinouts of the straight-through cable.

UTP straight-through pinouts

You can determine that the wiring is a straight-through cable by holding both ends of the

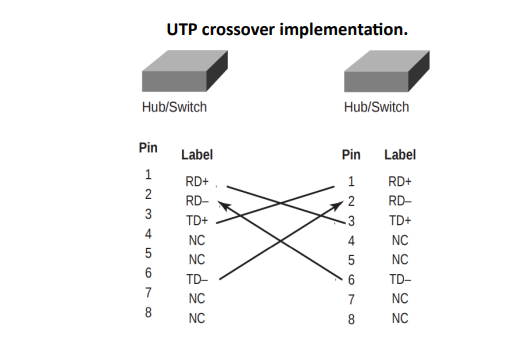
UTP cable side by side and seeing that the order of the wires on both ends is identical.

You can use a straight-through cable for the following tasks:

• Connecting a router to a hub or switch

• Connecting a server to a hub or switch

• Connecting workstations to a hub or switch



In the implementation of a crossover, the wires on each end of the cable are crossed.

Transmit to Receive and Receive to Transmit on each side, for both tip and ring.

UTP crossover implementation.

Notice that pin 1 on one side connects to pin 3 on the other side, and pin 2 connects to

pin 6 on the opposite end.

You can use a crossover cable for the following tasks:

• Connecting uplinks between switches

• Connecting hubs to switches

• Connecting a hub to another hub

• Connecting a router interface to another router interface

• Connecting two PCs together without a hub or switch

All Cisco devices are shipped with console cables and connectors, which allow you to

connect to a device and configure, verify, and monitor it. The cable used to connect

between a PC is a rollover cable with RJ-45 connectors.

The pinouts for a rollover cable are as follows:

1–8

2–7

3–6

4–5

5–4

6–3

7–2

8–1

You can see that you just take a straight-through RJ-45 cable, cut the end off, flip it over,

and reattach a new connector. Typically, you will use the DB9 connector to attach to your

PC and use a com port to communicate via HyperTerminal. Most Cisco devices now support RJ-45 console connections. However, the Catalyst 5000 series switch still uses a

DB25 connector. Set up the terminal emulation program to run 9600bps, 8 data bits, no

parity, 1 stop bit, and no flow control. On some routers, you need to verify that the

terminal emulation program is emulating a VT100 dumb-terminal mode, not an autosense mode, or it won’t work. Most routers also have an aux port, which is an auxiliary

port used to connect a modem. You can then dial this modem and connect the router to

the aux port. This will give you console access to a remote router that might be down

and that you cannot telnet into. The console port and aux port are considered out-ofband management since you are configuring the router “out of the network.” Telnet is

considered in-band.